Remarks

At present, the Examiner has objected to what he describes as being an undefined acronym in the Abstract. Applicant's abstract as originally presented provides no ambiguity whatsoever to those of ordinary skill in the subject art. To anyone engaged in the area of finite field operations, the term "GF" is just as much second nature as the term "RPM" is to an Indianapolis Speedway race driver. Nonetheless, applicant has amended the abstract to include the word 'Galois' to avoid any potential ambiguity.

Attention is next directed to the rejection of applicant's claims 1-4 under 35 U.S.C. § 103(a) based upon the patent to Golnabi et al. (US patent number 6,044,390 issued March 28, 2000). This rejection is respectfully traversed.

There are a number of very significant differences between applicant's claims and the teachings found in Golnabi et al. The similarities are merely superficial. For comparison sake, the Examiner's attention is directed to Figure 4 from the patent to Golnabi et al. and to Figure 6 from applicant's specification. The Examiner asserts that the multiplier U3 in Golnabi et al. is akin to the multiplier shown on the top of Figure 6. However, the teachings of Golnabi et al. clearly and unambiguously teach that one of the factors input to this multiplier is a field element a and that it is a fixed four bits in width. In this regard, it is to be particularly noted that even if it were 8 bits or 16 bits, the clear teachings of Golnabi et al. are that this is a fixed sized element. Not only is it fixed in size, it is fixed in its value. In stark contrast, it is to be noted that applicant's multiplier multiplies two polynomials and, furthermore, that this multiplication is modulo an irreducible polynomial p(x).

The Examiner goes on to assert that the summer U5 in Golnabi et al. is akin to the exclusive OR (modulo 2) summation shown in applicant's Figure 6. However, applicant's Figure

6 clearly shows that his summer includes only two inputs. In stark contrast, it is to be noted that Golnabi et al. teach that their U5 summer receives inputs from a multiplier U4, from a multiplier U3, and from a third source U2. In contrast, it is seen that applicant's summer (effectively the exclusive OR block shown) has only two inputs. Clearly, the output of summer U5 from Golnabi et al. is a value which is extraordinarily different than that which is produced by applicant's claims which closely track applicant's Figure 6.

There are yet other major differences between the art cited and applicant's claims. In particular, it is noted that the output of the summer U5 in Golnabi et al. is supplied to a register γ whose output is supplied to a multiplier U4. Let us assume for the moment, and solely for the sake of argument, that the U4 multiplier in Golnabi et al. is analogous to the block in applicant's Figure 6 which multiplies the output of register c(x) by x^n modulo the irreducible polynomial p(x). No such multiplication is carried out by the multiplier U4 in Golnabi et al. In particular, as in multiplier U3, Golnabi et al. clearly teach that one of the inputs for this multiplier must be a fixed field element α^2. And again, Golnabi et al. teach that this is a fixed four bit value, fixed not only in terms of the number of bits, but fixed also in terms of its value. Clearly, multiplication by a fixed field element α^2 is not the same as multiplication by x^n. Additionally, applicant's drawings and claims reflect the fact that this multiplication is a modulo and irreducible polynomial. This aspect does not appear to be part of the functioning of either multiplier U3 or multiplier U4 in the patent to Golnabi et al.

Accordingly, while it is seen that there are certain superficial similarities and analogous structures, it is clearly seen that the teachings of Golnabi et al. would not lead anyone of ordinary skill in the art to the invention described in applicant's claims and shown in applicant's Figure 6. Accordingly, it is therefore respectfully requested that the rejection of applicant's claims 1-4 under 35 U.S.C. § 103(a) be withdrawn.

It is noted that the current response does not require the payment of any additional fees.

Accordingly, it is now seen that all of the applicant's claims are in condition for allowance. Therefore, early notification of the allowability of applicant's claims is earnestly solicited. Furthermore, if there are any other matters which the Examiner feels could be expeditiously considered and which would forward the prosecution of the instant application, applicant's attorney wishes to indicate his willingness to engage in any telephonic communication in furtherance of this objective. Accordingly, applicant's attorney may be reached for this purpose at the numbers provided below.

Respectfully Submitted,

Date

LAWRENCE D. CUTTER, Senior Attorney
Reg. No. 28,501

IBM Corporation, IP Law Dept.
2455 South Rd., M/S P386
Poughkeepsie, NY 12601

Phone: (845) 433-1172
FAX: (845) 432-9786
EMAIL: cutter@us.ibm.com